

**PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE**

29.01.03.P0.13 Information Resources – Server Hardening

Approved (May 26, 2009)

Next Scheduled Review (May-2012)

1. PURPOSE

- 1.1 Servers are relied upon to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Prairie View A&M University has developed rules and procedures that address acceptable use of information resources. The purpose of this University Administrative Procedure (UAP) is to identify those relevant policies and procedures.

- 1.2 This UAP applies to all University information resources.

The purpose of the implementation of this UAP is to provide a set of measures that will mitigate information security risks associated with acceptable use of University information resources. There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures will be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this UAP based on information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer.

The intended audience for this UAP includes, but is not limited to, all information resources management personnel, owners, system administrators, and users of University information resources.

2. DEFINITIONS

- 2.1 Information Resources (IR): the procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.
- 2.2 Information Security Officer (ISO): responsible for administering the information security functions within Prairie View A&M University and reports to the Information

Resources Manager (IRM).

- 2.3 Confidential Information: information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act. .
- 2.4 Mission Critical Information: information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the university or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, and failure to comply with regulations or legal obligations, or closure of the University or department.
- 2.5 Owner of an Information Resource: an entity responsible for a business function and for determining controls and access to information resources supporting that business function.

3. PROCEDURES AND RESPONSIBILITIES

- 3.1 Systems administrators will test security patches prior to implementation.
- 3.2 System administrators shall ensure that vendor supplied patches are routinely acquired, systematically tested, and installed promptly.
- 3.3 System administrators shall remove unnecessary software, system services, and drivers.
- 3.4 System administrators shall enable security features included in vendor supplied systems including, but not limited to, firewalls, virus scanning and malicious code protections, and other file protections (see Malicious Code procedure). Audit logging shall also be enabled. User privileges shall be set utilizing the least privileges concept of providing the minimum amount of access required to perform job functions. The use of passwords shall be enabled in accordance with the University Password Policy.
- 3.5 System administrators shall disable or change the password of default accounts.
- 3.6 Servers shall be tested for known vulnerabilities when new vulnerabilities are announced, and shall seek and implement best practices for securing their particular system platform(s).

Contact Office: Information Security Officer; 936-261-2126